PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 20 April 2000 (20.04.00)	
International application No.: PCT/EP99/07051	Applicant's or agent's file reference: P98136WO.IP
International filing date: 22 September 1999 (22.09.99)	Priority date: 09 October 1998 (09.10.98)
Applicant: SCHWENK, Jörg	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

12 February 2000 (12.02.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

DEUTSCHE TELEKOM AG
Rechtsabteilung (Patente), PA1
D-64307 Darmstadt
ALLEMAGNE

Date of mailing (day/month/year)
10 March 2000 (10.03.00)

Applicant's or agent's file reference
P98136WO.IP

IMPORTANT NOTIFICATION

International application No.
PCT/EP99/07051

International filing date (day/month/year)
22 September 1999 (22.09.99)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [ ] the agent [X] the common representative

Name and Address

DEUTSCHE TELEKOM AG
Patentabteilung R151
D-64307 Darmstadt
Germany

State of Nationality:
State of Residence:
Telephone No.: 06151/83-58-42
Facsimile No.: 06151/83-58-43
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

DEUTSCHE TELEKOM AG
Rechtsabteilung (Patente), PA1
D-64307 Darmstadt
Germany

State of Nationality:
State of Residence:
Telephone No.: 06151/83-58-40
Facsimile No.: 06151/83-58-43
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
F. Baechler

Telephone No.: (41-22) 338.83.38

Deutsches Patent- und Markenamt

München, den 22. November 1999
Telefon: (0 89) 21 95 - 2516
Aktenzeichen: 198 47 941.7
Anmelder: s.Adr.

Deutsches Patent- und Markenamt · 80297 München

Deutsche Telekom AG
Technologiezentrum
Patentabteilung EK 03

64276 Darmstadt

Deutsche Telekom AG
Patentabteilung
Eing.: 29. NOV. 1999
PA1-2

Ihr Zeichen: P 98136

Bitte Aktenzeichen und Anmelder bei allen Eingaben und Zahlungen angeben

Zutreffendes ist angekreuzt ☒ und/oder aus ausgefüllt!

Ergebnis einer Druckschriftenermittlung

Auf den Antrag des
wirksam am 9.Okt. 1998 gemäß ☒ § 43 Patentgesetz ☐ § 7 Gebrauchsmustergesetz
sind die auf den beigefügten Anlagen angegebenen öffentlichen Druckschriften ermittelt worden.
Ermittelt wurde in folgenden Patentklassen:

Klasse/Gruppe	Prüfer	Patentabt.
H04L 9/30,00,32,12/44,G06F 17/30	Süßmuth	31

Best Available Copy

Die Recherche im Deutschen Patent- und Markenamt stützt sich auf die Patentliteratur folgender Länder und Organisationen:

Deutschland (DE,DD), Österreich, Schweiz, Frankreich, Großbritannien, USA, Japan (Abstracts), UDSSR (Abstracts), Europäisches Patentamt, WIPO.

Recherchiert wurde außerdem in folgenden Datenbanken:

Anlagen:
Anlagen 1, 2 und 3 zur Mitteilung der ermittelten Druckschriften

6 Druckschrift(en) bzw. Ablichtung(en)

Patentabteilung 11
Recherchen-Leitstelle

EL302703835

198 47 941.7

Deutsches Patent- und Markenamt · 80297 München

Anlage 1

zur Mitteilung über die ermittelten Druckschriften
gemäß § 43 des Patentgesetzes

Druckschriften:

DE	196 49 292 A1	DE	195 11 298 A1
US	46 61 658	US	43 09 569
EP	03 14 292 B1		

Literatur:

JP 05327748 A., In: Patent Abstracts of Japan;

Für den Anmelder / Antragsteller

Deutsches Patent- und Markenamt

80297 München

Anlage 2

zur Mitteilung der ermittelten Druckschriften

Aktenzeichen
198 47 941.7

Erläuterungen zu den ermittelten Druckschriften:

1 ~~Kategorie~~ Category	2 ~~Ermittelte Druckschriften/Erläuterungen~~ Printed Reference / Explanation			3 ~~Betrifft Anspruch~~ Claims
X	US	46 61 658	Fig. 2 ~~mit Beschr.~~ with Description	1,2
Y	DE	196 49 292 A1	Anspr. 1	1,2
A	DE	195 11 298 A1		
A	EP	03 14 292 B1		
Y	US	43 09 569	~~Sp~~.3, ~~Z~~. 41-49, Fig. 1 (col. lines)	1
Y	JP 05327748 A., In: Patent Abstracts of Japan; Fig. 1 ~~mit Abstr~~. (with abstract)			1

Erklärungen siehe Anlage 3 (P 2255)

Best Available Copy

Deutsches Patent- und Markenamt

Anlage 3

zur Mitteilung der ermittelten Druckschriften

Hinweise zur Mitteilung (Vordruck P 2251)

Eine Gewähr für die Vollständigkeit der Ermittlung wird nicht geleistet (§ 43 Abs. 7 Patentgesetz bzw. § 7 Abs. 2 Gebrauchsmustergesetz i.V.m. § 43 Abs. 7 Satz 1 Patentgesetz).

Die angegebene Patentliteratur kann in den Auslegehallen des Deutschen Patent- und Markenamts, 80331 München, Zweibrückenstraße 12, oder 10969 Berlin, Gitschiner Str. 97 eingesehen werden; deutsche Patentschriften, Auslegeschriften und Offenlegungsschriften auch in den Patentinformationszentren. Ein Verzeichnis über diese Patentinformationszentren kann auf Wunsch vom Deutschen Patent- und Markenamt sowie von einigen Privatfirmen bezogen werden.

Erklärungen zur Anlage 2 (Vordruck P 2253)

Spalte 1: Kategorie

Es bedeutet:

- **X:** Druckschriften, die Neuheit oder Erfindungshöhe allein in Frage stellen
- **Y:** Druckschriften, die die Erfindungshöhe zusammen mit anderen Druckschriften in Frage stellen
- **A:** Allgemein zum Stand der Technik, technologischer Hintergrund
- **O:** Nicht-schriftliche Offenbarung, z.B. ein in einer nachveröffentlichten Druckschrift abgedruckter Vortrag,der vor dem Anmelde- oder Prioritätstag öffentlich gehalten wurde
- **P:** Im Prioritätsintervall veröffentlichte Druckschriften
- **T:** Nachveröffentlichte, nicht kollidierende Druckschriften, die die Theorie der angemeldetenErfindung betreffen und für ein besseres Verständnis der angemeldeten Erfindung nützlich sein können bzw. zeigen, daß der angemeldeten Erfindung zugrunde liegende Gedankengänge oder Sachverhalte falsch sein könnten
- **E:** Ältere Anmeldungen gemäß § 3 Abs. 2 PatG (bei Recherchen nach § 43 PatG); ältere Patentanmeldungen oder ältere Gebrauchsmuster gemäß § 15 GbmG (bei Recherchen nach § 7 GbmG)
- **D:** Druckschriften, die bereits in der Patentanmeldung genannt sind
- **L:** Aus besonderen Gründen genannte Druckschriften, z.B. zum Veröffentlichungstag einer Entgegenhaltung oder bei Zweifeln an der Priorität.

Spalte 2: Ermittelte Druckschriften / Erläuterungen

- **Veröff.:** Veröffentlichungstag einer Druckschrift im Prioritätsintervall
- **nr:** Nicht recherchiert, da allgemein bekannter Stand der Technik, oder nicht recherchierbar
- **=:** Druckschriften, die auf dieselbe Ursprungsanmeldung zurückgehen ("Patentfamilien") oder auf die sich Referate oder Abstracts beziehen.
- **"-":** Nichts ermittelt

Spalte 3: Betroffene Ansprüche

Hier sind die Ansprüche unter Zuordnung zu den in Spalte 2 genannten relevanten Stellen angegeben.

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

PCT/EP 99 / 07051
Internationales Aktenzeichen

(22. 09. 1999) 22 SEP 1999
Internationales Anmeldedatum

EUROPEAN PATENT OFFICE
PCT INTERNATIONAL APPLICATION
Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)* P98136WO.1P

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

DEUTSCHE TELEKOM AG
Friedrich-Ebert-Allee 140

53113 Bonn
Deutschland

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

SCHWENK; Jörg
Südwestring 27

64807 Dieburg
DE

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nichtnötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☐ Anwalt ☒ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Deutsche Telekom AG
Patentabteilung R151
64307 Darmstadt
Deutschland

Telefonnr.: 06151/83-58 42

Telefaxnr.: 06151/83-58 43

Fernschreibnr.:

☐ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Siehe Anmerkungen zu diesem Antragsformular

EL302703835 45

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☐ **AP** **ARIPO-Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenia, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SL** Sierra Leone, **SZ** Swasiland, **UG** Uganda, **ZW** Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☐ **EA** **Eurasisches Patent:** **AM** Armenien, **AZ** Aserbaidschan, **BY** Belarus, **KG** Kirgisistan, **KZ** Kasachstan, **MD** Republik Moldau, **RU** Russische Föderation, **TJ** Tadschikistan, **TM** Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ **EP** **Europäisches Patent:** **AT** Österreich, **BE** Belgien, **CH und LI** Schweiz und Liechtenstein, **CY** Zypern, **DE** Deutschland, **DK** Dänemark, **ES** Spanien, **FI** Finnland, **FR** Frankreich, **GB** Vereinigtes Königreich, **GR** Griechenland, **IE** Irland, **IT** Italien, **LU** Luxemburg, **MC** Monaco, **NL** Niederlande, **PT** Portugal, **SE** Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☐ **OA** **OAPI-Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Zentralafrikanische Republik, **CG** Kongo, **CI** Côte d'Ivoire, **CM** Kamerun, **GA** Gabun, **GN** Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauretanien, **NE** Niger, **SN** Senegal, **TD** Tschad, **TG** Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☐ **AE** Vereinigte Arabische Emirate
- ☐ **AL** Albanien .....
- ☐ **AM** Armenien .....
- ☐ **AT** Österreich .....
- ☐ **AU** Australien .....
- ☐ **AZ** Aserbaidschan
- ☐ **BA** Bosnien-Herzegowina .....
- ☐ **BB** Barbados
- ☐ **BG** Bulgarien .....
- ☐ **BR** Brasilien .....
- ☐ **BY** Belarus .....
- ☐ **CA** Kanada
- ☐ **CH und LI** Schweiz und Liechtenstein
- ☐ **CN** China .....
- ☐ **CU** Kuba .....
- ☐ **CZ** Tschechische Republik .....
- ☐ **DE** Deutschland .....
- ☐ **DK** Dänemark .....
- ☐ **EE** Estland .....
- ☐ **ES** Spanien .....
- ☐ **FI** Finnland .....
- ☐ **GB** Vereinigtes Königreich
- ☐ **GD** Grenada
- ☐ **GE** Georgien .....
- ☐ **GH** Ghana .....
- ☐ **GM** Gambia
- ☐ **HR** Kroatien .....
- ☒ **HU** Ungarn .....
- ☐ **ID** Indonesien
- ☒ **IL** Israel .....
- ☐ **IN** Indien .....
- ☐ **IS** Island
- ☒ **JP** Japan .....
- ☐ **KE** Kenia .....
- ☐ **KG** Kirgisistan .....
- ☐ **KP** Demokratische Volksrepublik Korea .....
- ☐ **KR** Republik Korea .....
- ☐ **KZ** Kasachstan .....
- ☐ **LC** Saint Lucia
- ☐ **LK** Sri Lanka
- ☐ **LR** Liberia
- ☐ **LS** Lesotho .....
- ☐ **LT** Litauen
- ☐ **LU** Luxemburg
- ☐ **LV** Lettland
- ☐ **MD** Republik Moldau .....
- ☐ **MG** Madagaskar .....
- ☐ **MK** Die ehemalige jugoslawische Republik Mazedonien .....
- ☐ **MN** Mongolei
- ☐ **MW** Malawi .....
- ☐ **MX** Mexiko .....
- ☐ **NO** Norwegen
- ☐ **NZ** Neuseeland .....
- ☐ **PL** Polen .....
- ☐ **PT** Portugal .....
- ☐ **RO** Rumänien
- ☐ **RU** Russische Föderation .....
- ☐ **SD** Sudan
- ☐ **SE** Schweden
- ☐ **SG** Singapur
- ☐ **SI** Slowenien .....
- ☐ **SK** Slowakei .....
- ☐ **SL** Sierra Leone .....
- ☐ **TJ** Tadschikistan .....
- ☐ **TM** Turkmenistan .....
- ☐ **TR** Türkei .....
- ☐ **TT** Trinidad und Tobago .....
- ☐ **UA** Ukraine .....
- ☐ **UG** Uganda .....
- ☒ **US** Vereinigte Staaten von Amerika .....
- ☐ **UZ** Usbekistan .....
- ☐ **VN** Vietnam .....
- ☐ **YU** Jugoslawien .....
- ☐ **ZA** Südafrika .....
- ☐ **ZW** Simbabwe .....

Kästchen für die Bestimmung von Staaten, die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☐ .....
- ☐ .....

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Feld Nr. VI PRIORITÄTSANSPRUCH ☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine: nationale Anmeldung: Staat	regionale Anmeldung:* regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 09.Oktober 1998 (09.10.1998)	19847941.7	DE		
Zeile (2)				
Zeile (3)				

☐ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln *(nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)*

* *Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.*

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) *(falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden):*

ISA / EP

Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche *(falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist):*

Datum *(Tag/Monat/Jahr)* Aktenzeichen Staat *(oder regionales Amt)*

Feld Nr. VIII KONTROLLISTE; EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält die folgende **Anzahl von Blättern:**

Antrag	: 4
Beschreibung (ohne Sequenzprotokollteil)	: 7
Ansprüche	: 2
Zusammenfassung	: 1
Zeichnungen	: 3
Sequenzprotokollteil der Beschreibung	: —
Blattzahl insgesamt	: 17

Dieser internationalen Anmeldung **liegen** die nachstehend angekreuzten Unterlagen **bei:**

1. ☒ Blatt für die Gebührenberechnung
2. ☐ Gesonderte unterzeichnete Vollmacht
3. ☒ Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden): 38692
4. ☐ Begründung für das Fehlen einer Unterschrift
5. ☐ Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer gekennzeichnet:
6. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:
7. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
8. ☐ Protokoll der Nucleotid- und/oder Aminosäuresequenzen in computerlesbarer Form
9. ☐ Sonstige *(einzeln aufführen):* Zusatzblatt

Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.): 1

Sprache, in der die internationale Anmeldung eingereicht wird: deutsch

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Deutsche Telekom AG

i.A. Rolf Henn

..... Fortsetzung Blatt 4

Rolf Henn, Referent der Patentabteilung
EPA-Vollmacht 38692

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung: (22.09.99) 22 SEP 1999

2. Zeichnungen ☒ eingegangen: ☐ nicht eingegangen:

3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:

4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:

5. Internationale Recherchenbehörde *(falls zwei oder mehr zuständig sind):* ISA /

6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Zusatzfeld *Wird dieses Zusatzfeld nicht benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.*

1. Wenn der ***Platz in einem Feld nicht für alle Angaben ausreicht****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. ..." [Nummer des Feldes angeben] und machen die Angaben entsprechend der in dem Feld, in dem der Platz nicht ausreicht, vorgeschriebenen Art und Weise, insbesondere:*

(i) ***Wenn mehr als zwei Anmelder und/oder Erfinder vorhanden sind*** *und kein "Fortsetzungsblatt" zur Verfügung steht: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. III" und machen für jede weitere Person die in Feld Nr. III vorgeschriebenen Angaben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.*

(ii) Wenn in Feld Nr. II oder III die Angabe ***"die im Zusatzfeld angegebenen Staaten"*** *angekreuzt ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Anmelders oder die Namen der Anmelder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Anmelder ist.*

(iii) Wenn der in Feld Nr. II oder III genannte ***Erfinder oder Erfinder/Anmelder nicht für alle Bestimmungsstaaten oder für die Vereinigten Staaten von Amerika als Erfinder benannt ist****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Erfinders oder die Namen der Erfinder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Erfinder ist.*

(iv) Wenn zusätzlich zu dem Anwalt oder den Anwälten, die in Feld Nr. IV angegeben sind, ***weitere Anwälte*** *bestellt sind: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. IV" und machen für jeden weiteren Anwalt die entsprechenden, in Feld Nr. IV vorgeschriebenen Angaben.*

(v) Wenn in Feld Nr. V bei einem Staat (oder bei OAPI) die Angabe ***"Zusatzpatent"*** *oder* ***"Zusatzzertifikat,"*** *oder wenn in Feld Nr. V bei den Vereinigten Staaten von Amerika die Angabe* ***"Fortsetzung"*** *oder* ***"Teilfortsetzung"*** *hinzugefügt wird: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. V" und geben den Namen des betreffenden Staats (oder OAPI) an und nach dem Namen jedes solchen Staats (oder OAPI) das Aktenzeichen des Hauptschutzrechts oder der Hauptschutzrechtsanmeldung und das Datum der Erteilung des Hauptschutzrechts oder der Einreichung der Hauptschutzrechtsanmeldung.*

(vi) Wenn in Feld Nr. VI ***die Priorität von mehr als drei früheren Anmeldungen beansprucht wird****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und machen für jede weitere frühere Anmeldung die entsprechenden, in Feld Nr. VI vorgeschriebenen Angaben.*

(vii) Wenn in Feld Nr. VI die ***frühere Anmeldung eine ARIPO Anmeldung*** *ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und geben, unter Angabe der Nummer der Zeile, in der die die frühere Anmeldung betreffenden Angaben gemacht sind, mindestens einen Staat an, der Mitglied der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung erfolgte.*

2. Wenn, im Hinblick auf die ***Erklärung bzgl. vorsorglicher Bestimmungen*** *in Feld Nr. V, der Anmelder Staaten von dieser Erklärung ausnehmen möchte: In diesem Fall schreiben Sie "Bestimmung(en), die von der Erklärung bzgl. vorsorglicher Bestimmungen ausgenommen ist(sind)" und geben den Namen oder den Zweibuchstaben-Code jedes so ausgeschlossenen Staates an.*

3. Wenn der Anmelder für irgendein Bestimmungsamt die Vorteile nationaler Vorschriften betreffend ***unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit*** *in Anspruch nimmt: In diesem Fall schreiben Sie "Erklärung betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit" und geben im folgenden die entsprechende Erklärung ab.*

Die Unterschrift des Erfinders bzw. Anmelders und die Prioritätsbescheinigung wird nachgereicht.

T5

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
P98136WO.IP		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/07051	22/09/1999	09/10/1998
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
H01L9/08		
Anmelder		
DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
12/02/2000	01.08.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Zucka, G Tel. Nr. +31 70 340 4026

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/07051

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,2,4-7	ursprüngliche Fassung			
3,3a	eingegangen am	16/06/2000	mit Schreiben vom	15/06/2000

Patentansprüche, Nr.:

3	ursprüngliche Fassung			
1,2	eingegangen am	16/06/2000	mit Schreiben vom	15/06/2000

Zeichnungen, Blätter:

1/3-3/3	ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-3
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-3
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-3
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

Zu Punkt V

1 Es wird auf das folgende Dokument verwiesen:

D1 = DAVID A. MCGREW AND ALAN T. SHERMAN: 'Key establishment in large dynamic groups using one-way function trees', 20. Mai 1998 (1998-05-20), Seiten 1-13; verfügbar auf Internet: <http://www.cs.umbc.edu/~sherman/Papers/it se.ps> 23. Juni 1998 XP002126220

2.1 Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des unabhängigen Anspruchs 1 angesehen. Es offenbart ein Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer, bei dem jedem der n Teilnehmer jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und in etwa die Tiefe $\lceil \log_2 n \rceil$ besitzt, zugeordnet wird.

2.2 Damit auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können, sieht das Verfahren der Anmeldung vor,

- daß jeder Teilnehmer selbst ein Geheimnis generiert und dieses dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer zugeordnet ist;

- daß nacheinander in Richtung der Baumwurzel für alle Knoten des Baumes Geheimnisse etabliert werden, wobei ausgehend von den Blättern entsprechend der festgelegten Baumstruktur über die gesamte Hierarchie der Baumstruktur immer zwei bereits bekannte Geheimnisse über das Diffie-Hellmann-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt und einem gemeinsamen Knoten zu geordnet werden, so daß der letzte Knoten und damit die Baumwurzel als Geheimnis den gemeinsamen Schlüssel aller n Teilnehmer enthält.

2.3 Eine solche Vorgehensweise wird von den im Recherchenbericht erwähnten Dokumente weder offenbart noch nahegelegt: beim Verfahren im Dokument D1

wird zur Etablierung des gemeinsamen Schlüssels ein "Group Manager" benötigt.

2.4 Die erfinderische Tätigkeit wird somit anerkannt.

3. Die Ansprüche 2-3 sind vom Anspruch 1 abhängig, und deren Gegenstand ist deshalb auch neu und erfinderisch.

4. Der Gegenstand der Ansprüche 1-3 ist gewerblich anwendbar.

Zu Punkt VII

1. Wenn D1 als nächstliegender Stand der Technik betrachtet wird, ist die Beschreibung der Erfindung auf Seite 3a, Zeile 10 - Seite 4, Zeile 4 nicht korrekt (Regel 5.1(a)(iii) PCT), weil auch in D1 das Etablieren eines Gruppenschlüssels mit Hilfe einer Baumstruktur vorgenommen wird, und die Anzahl der an der Schlüsselbildung beteiligten Teilnehmer n als binärer Baum mit n Blättern dargestellt wird, wobei jedem Teilnehmer ein Blatt des binären Baumes mit der Tiefe $\lceil \log_2 n \rceil$ zugeordnet ist.

2. Aus dem gleichen Grund ist auch die zweiteilige Form nicht korrekt (Regel 6.3(b) PCT).

Bei allen diesen Erweiterungen tritt mindestens eines der drei folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z. B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Unter dem Titel „Key estalishment in large dynamic groups using one-way function trees" von David A. McGrew und Alan T. Sherman wurde bei den IEEE Transaction On Software Engineering ein Artikel vom 20.05 1998 Seite 1 bis 13 eingereicht, der ebenfalls ein Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels vorstellt. Dieses Verfahren basiert auf einer Baumstruktur. Ein Gruppenmanager (Group Manager) verwaltet dabei einen Binärbaum, wobei jeder Knoten x von ihm mit zwei kryptografischen Schlüsseln verknüpft ist, einem Knotenschlüssel kx und einem verdeckten Knotenschlüssel $k'x \approx g(k_x)$. Der verdeckte Knotenschlüssel wird aus dem Knotenschlüssel mit Hilfe einer Einwegfunktion berechnet. Jeder Teilnehmer kennt die unverdeckten Knotenschlüssel auf dem Pfad von seinem Knoten bis zur Wurzel und die verdeckten Knotenschlüssel für die Knoten, die für seinen Pfad zur Root Geschwister sind und sonst keine anderen verdeckten oder unverdeckten Schlüssel. Die Durchführbarkeit dieses Verfahrens beruht offensichtlich darauf, dass der Gruppenmanager alle Blatt-Schlüssel kennt.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT`94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000 Bit gesendet werden müssen.

Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptografisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert

werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren soll das Etablieren eines gemeinsamen Gruppenschlüssels zwischen einer Zentrale und einer Gruppe von n Teilnehmern ermöglichen . Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können.

Die Aufgabenstellung wird durch ein Verfahren gelöst, bei welchem das Etablieren eines Gruppenschlüssels mit Hilfe einer Baumstruktur vorgenommen wird. Dazu wird die Anzahl der an der Schlüsselvereinbarung beteiligten Teilnehmer n als binärer Baum mit n Blättern dargestellt. Für jede natürliche Zahl n gibt es eine oder mehrere

(3) Patentansprüche:

1. Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer unter Anwendung des an sich bekannten DH-Verfahrens, bei dem jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und in etwa die Tiefe $\lceil \log_2 n \rceil$ besitzt, zugeordnet wird,
dadurch gekennzeichnet,
-daß jeder Teilnehmer (I) selbst ein Geheimnis (i) generiert und dieses dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist,
-daß nacheinander in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert werden, wobei ausgehend von den Blättern entsprechend der festgelegten Baumstruktur über die gesamte Hierarchie der Baumstruktur immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt und einem gemeinsamen Knoten (K) zu geordnet werden, so daß der letzte Knoten K_W und damit die Baumwurzel als Geheimnis den gemeinsamen Schlüssel aller n Teilnehmer enthält.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,**
-daß bei Aufnahme eines neuen Teilnehmers in eine bestehende Baumstruktur, die bereits über ein gemeinsames Geheimnis verfügt, zum Etablieren eines gemeinsamen Schlüssels für n+1 Teilnehmer an geeigneter Stelle des binären Baumes einem Blatt (B) als Nachfolger zwei neue Blätter (B1 und B2) angefügt werden, so daß der neue Baum genau n+1 Blätter und die Tiefe $\lceil \log_2(n+1) \rceil$ besitzt,
-daß der dem bisherigen Blatt (B) zugeordnete Teilnehmer und der neue Teilnehmer jeweils einem der neuen Blätter (B1; B2) zugeordnet werden, wobei das bisherige Blatt B zu einem gemeinsamen Knoten für die neuen Blätter (B1;B2) wird,
-daß ausgehend von den neuen Blättern (B1;B2) bis zur Wurzel des Baumes nur in den Knoten neue Geheimnisse etabliert werden, die im Rahmen der Baumstruktur auf dem Weg von den Blättern B1 und B2 zur Baumwurzel liegen.

09/807181

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

3

Applicant's or agent's file reference P98136WO.IP	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/07051	International filing date (*day/month/year*) 22 September 1999 (22.09.99)	Priority date (*day/month/year*) 09 October 1998 (09.10.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant DEUTSCHE TELEKOM AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12 February 2000 (12.02.00)	01 August 2000 (01.08.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/07051

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☒ the international application as originally filed.

☒ the description, pages 1,2,4-7, as originally filed,
pages _____, filed with the demand,
pages 3,3a, filed with the letter of 15 June 2000 (15.06.2000),
pages _____, filed with the letter of _____.

☒ the claims, Nos. 3, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1,2, filed with the letter of 15 June 2000 (15.06.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/3 - 3/3, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-3	YES
	Claims		NO
Inventive step (IS)	Claims	1-3	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-3	YES
	Claims		NO

2. Citations and explanations

1. This report makes reference to the following document:

D1: DAVID A. MCGREW AND ALAN T. SHERMAN: "Key establishment in large dynamic groups using one-way function trees", 20 May 1998 (1998-05-20), pages 1-13; available on the internet: http://www.cs.umbc.edu/~sherman/Papers/itse.ps 23 June 1998, XP002126220.

2.1 Document D1 is considered the prior art closest to the subject matter of independent Claim 1 and discloses a method for establishing a shared cryptographic key for n subscribers, in which method each of the n subscribers is associated with a leaf of a binary tree having exactly n leaves and approximately the length $\lceil \log_2 n \rceil$.

2.1 For subscribers to be evicted from or added to the key directory without much outlay, even after the group key has been established, the claimed method proposes that

- each subscriber generates himself a secret and this is associated with the tree leaf which is also associated with the subscriber in question;

- secrets are successively established in the direction of the tree roots for all nodes of the tree, starting from the leaves and continuing through the entire hierarchy of the tree structure, according to the determined tree structure, every two already known secrets being combined by the Diffie-Hellmann method into a new shared secret and associated with a shared node, so that the last node and hence the tree root contains as a secret the shared key of all n subscribers.

2.3 Th search report citations neither disclose nor suggest such a procedure. In the method of D1, a "group manager" is required for establishing the shared key.

2.4 Inventive step is therefore acknowledged.

3. Claims 2-3 are dependent on Claim 1 and their subject matter is therefore also novel and inventive.

4. The subject matter of Claims 1-3 is industrially applicable.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. If D1 is considered the closest prior art, then the description of the invention on page 3a, line 10 to page 4, line 4, is not correct (PCT Rule 5.1(a)(iii)) because a group key is also established in D1 by means of a tree structure and the number of n subscribers which participate in forming the key is also represented as a binary tree with n leaves, each subscriber being associated with one leaf of the binary tree having the length $\lceil \log_2 n \rceil$.

2. For the same reason, the two-part form is also incorrect (PCT Rule 6.3(b)).

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International Reference PCT/EP99/07051

I. Basis of the report

1. This report has been prepared on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments):*

the Specification, pages

1,2,4-7	as originally filed
3,3a	received on 6/16/00 with letter of 6/15/00

the Claims, nos.

3	as originally filed
1,2	received on 6/16/00 with letter of 6/15/00

the Drawings, sheets/fig.

1/3-3/3	as originally filed

V. Substantiated determination according to Article 35(2) with respect to novelty, inventive activity and industrial applicability; documents and clarifications in support of this determination

1. DETERMINATION

Novelty	Claims 1-3	YES
	Claims	NO
Inventive Activity	Claims 1-3	YES
	Claims	NO
Industrial Applicability	Claims 1-3	YES
	Claims	NO

2. DOCUMENTS AND CLARIFICATIONS

See Supplementary Page.

EL302703835

EL302703833US

Best Available Copy

VII. Specific Shortcomings of the International Application

It was determined that the International Application has the following shortcomings with regard to form or content:

See Supplementary Page

Re Point V

1 Reference is made to the following document:

D1 = DAVID A. MCGREW AND ALAN T. SHERMAN: "*Key Establishment in Large Dynamic Groups Using One-Way Function Trees*", May 1998 (5/20/1998), pages 1-13; available on the Internet: <http://www.cs.umbc.edu/~sherman/Papers/itse.ps >23.June 1998 XP002126220

2.1 Document D1 is regarded as the most proximate related art with respect to the subject matter of the independent Claim 1. It discloses a process for establishing a common cryptographic key for n subscribers, in which each of the n subscribers is assigned one leaf of a binary-structured tree that has exactly n leaves and is, let us say, of depth $\lceil \log_2 n \rceil$.

2.2 In order to be able to delete from or add subscribers to the key directory without great effort even after the group key has been established, the method of the present Application provides that:

- each subscriber him/herself generates a secret which is assigned to that leaf of the tree to which the respective subscriber is also assigned;

- secrets are established consecutively in the direction of the tree root for all nodes of the tree, where starting from the leaves **[and]** according

to the defined tree structure across the entire hierarchy of the tree structure, two already known secrets are always combined via the Diffie-Hellmann process to form a new common secret and are allocated to a common node, so that the last node and therefore the tree root contains the common key of all n subscribers as the secret.

2.3 Such a procedure is neither disclosed nor suggested by the documents mentioned in the Search Report: In the case of the method in document D1, a "group manager" is needed for establishing the common key.

2.4 The inventive activity is thus acknowledged.

3. Claims 2-3 are dependent on Claim 1, and their subject matter is therefore also novel and inventive.

4. The subject matter of Claims 1-3 is industrially applicable.

Re Point VII

1. If D1 is considered as the most proximate related art, the description of the invention on page 3a, line 10 - page 4, line 4 is not correct (Rule 5.1(a)(iii)PCT), because a group key is established with the aid of a tree structure in D1, as well, and the number of subscribers n involved in forming the key is represented as a binary tree having n leaves, one leaf of the binary tree having the depth $\lceil \log_2 n \rceil$ being allocated to each subscriber.

2. The two-part form is also not correct for the same reason (Rule 6.3(b) PCT).

In all these extensions, at least one of the following three problems occurs:

- The subscribers must be arranged in a certain manner, for instance in a circle in the above example.
- The subscribers have no influence vis-à-vis the central station on the choice of key.
- The number of rounds is dependent on the number of subscribers.

A further process for the common establishment of a key is known from the German Patent 195 38 385.0. In this process, however, the central station must know the secret keys of the subscribers.

In the IEEE Transaction On Software Engineering, an article dated 5/20/1998, pages 1 through 13, was submitted under the title *"Key Establishment in Large Dynamic Groups Using One-Way Function Trees"* by David A. McGrew and Alan T. Sherman, which likewise introduces a process for establishing a common cryptographic key. This process is based on a tree structure. In that case, a group manager manages a binary tree, each node x of it being linked to two cryptographic keys, a node key kx and a hidden node key $k'x \approx g(k_x)$. The hidden node key is calculated from the node key with the aid of a one-way function. Each subscriber knows the unhidden node keys on the path from his/her node up to the root and the hidden node keys for the nodes which are siblings for his/her path to the root, and otherwise no other hidden or unhidden keys. The feasibility of this process is obviously based on the fact that the group manager knows all the leaf keys.

A design approach from Burmester, Desmedt, *A secure and*

efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 is also known, in which two rounds are required to generate the key, it being necessary in the second round for the central station to send n messages of length p = approx. 1000 bits for n subscribers.

Also known is a cryptographic process referred to as the (n,t) threshold process. With an (n,t) threshold process, it is possible to break a key k down into t parts (called shadows), such that said key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Verlag, Wiesbaden 1998).

The present process is intended to permit the establishment of a common group key between a central station and a group of n subscribers. The process is to be such that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

The objective is achieved by a process in which a group key is established with the aid of a tree structure. To that end, the number of subscribers n involved in the key agreement is represented as a binary tree having n leaves. For each natural number n, there are one or more...

New Patent Claims

1. A process for establishing a common cryptographic key for n subscribers using the DH process which is known per se, in which each of the n subscribers (I) is assigned one leaf of a binary-structured tree which has precisely n leaves and is, let us say, of depth $\lceil \log_2 n \rceil$
characterized in that,
- each subscriber (I) him/herself generates a secret (i) which is assigned to that leaf of the tree to which the respective subscriber (I) is also assigned;
- secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, where starting from the leaves according to the defined tree structure across the entire hierarchy of the tree structure, two already known secrets are always combined via the DH process to form a new common secret and are allocated to a common node (K), so that the last node K_w and therefore the tree root contains the common key of all n subscribers as the secret.

2. The process as recited in Claim 1,
characterized in that
- when a new subscriber is added to an existing tree structure which already has a common secret, in order to establish a common key for n+1 subscribers, two new leaves (B1 and B2) are added as successors to a leaf (B) at a suitable location of the binary tree, so that the new tree has precisely n+1 leaves and is of depth $\lceil \log_2 (n+1) \rceil$;
- the subscriber assigned to the previous leaf (B) and the new subscriber are each assigned to one of the new leaves (B1;B2), the previous leaf B becoming a common node for the new leaves (B1;B2);
- starting from the new leaves (B1;B2) and going as far as the root of the tree, new secrets are established only in those nodes which lie within the framework of the tree

structure on the path from leaves B1 and B2 to the tree root.

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: WO 00/22775
H04L 9/08	A1	(43) Internationales Veröffentlichungsdatum: 20. April 2000 (20.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07051

(22) Internationales Anmeldedatum: 22. September 1999 (22.09.99)

(30) Prioritätsdaten:
198 47 941.7 9. Oktober 1998 (09.10.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHWENK, Jörg [DE/DE]; Südwestring 27, D-64807 Dieburg (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Rechtsabteilung (Patente), PA1, D-64307 Darmstadt (DE).

(81) Bestimmungsstaaten: HU, IL, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

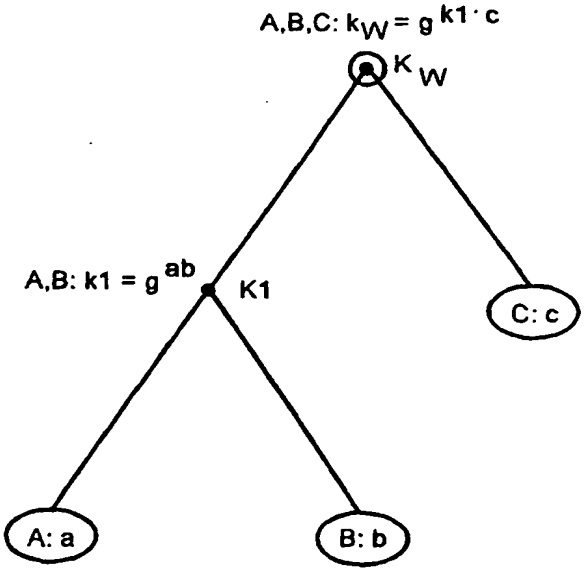
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

(54) Bezeichnung: VERFAHREN ZUM ETABLIEREN EINES GEMEINSAMEN KRYPTOGRAFISCHEN SCHÜSSELS FÜR N TEILNEHMER

(57) Abstract

The aim of the invention is to provide a method which also enables subscribers to be easily deleted from or added to the key directory after the group key has been established. According to the invention, a terminal node of a binary-structured tree is allocated to each of the n subscribers (I), said tree having exactly n terminal nodes and having a depth [$\log_2 n$]. A secret (i) is generated for each subscriber (I) and allocated to the particular terminal node of the tree to which the subscriber (I) is allocated. Secrets are then established for all of the nodes (K) of the tree in succession, in the direction of the roots of the tree. Two already known secrets are always amalgamated into one new, joint secret using the DH method. The last node K_W contains the joint key for all n subscribers. The inventive method can be used particularly advantageously for producing a cryptographic key for a group of subscribers whose number is subject to changes.



(57) Zusammenfassung

Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können. Erfindungsgemäß wird jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe [$\log_2 n$] besitzt, zugeordnet. Für jeden Teilnehmer (I) wird ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist. Nacheinander werden in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert, wobei immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeisamen Geheimnis zusammengefaßt werden. Der letzte Knoten K_W enthält den gemeinsamen Schlüssel aller n Teilnehmer. Das erfindungsgemäße Verfahren läßt sich vorteilhaft zur Erzeugung eines kryptografischen Schlüssels für eine Gruppe von Teilnehmern einsetzen, deren Teilnehmerzahl Änderungen unterworfen ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer

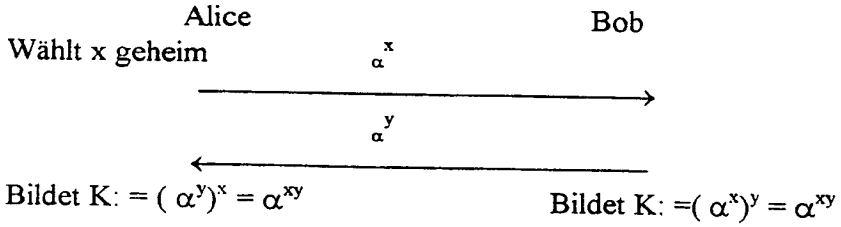
Beschreibung:

Das erfindungsgemäße Verfahren dient der Erzeugung und dem Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer zur Gewährleistung der Geheimhaltung von Nachrichten, die über unsichere Kommunikationskanäle ausschließlich an die n Teilnehmer übertragen werden sollen.

Zum Schutz der Vertraulichkeit und Integrität der Kommunikation zwischen zwei oder mehr Personen werden die Mechanismen der Verschlüsselung und Authentisierung eingesetzt. Diese erfordern allerdings das Vorhandensein einer gemeinsamen Information bei allen Teilnehmern. Diese gemeinsame Information wird als kryptographischer Schlüssel bezeichnet.

Ein bekanntes Verfahren zum Etablieren eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist das Verfahren von Diffie und Hellman (DH-Verfahren; vergleiche W. Diffie und M. Hellman, New Directions in Cryptography, IEEETransactions on Information Theory, IT-22(6):644-654, November 1976).

Grundlage des Diffie-Hellmann-Schlüsselaustauschs (DH76) ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren mit x bzw. y einen gemeinsamen Schlüssel $K := \alpha^{xy}$ berechnen. Ein Angreifer, der nur α^x und α^y sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z. B. von α^x zur Basis α modulo p zu berechnen und dann α^y damit zu potenzieren.)



Beispiel für Diffie-Hellmann-Schlüsselaustausch

Das Problem bei dem im Beispiel beschriebenen DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob oder mit einem Betrüger kommuniziert. In IPSec wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z. B. mit endlichen Körpern GF(2^n) oder elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern. Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.

Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). (Einen Überblick über den Stand der Technik bietet M. Steiner, G. Tsudik, M. Waidner, Diffie-Hellman Key Distribution Extended to Group Communication. Proc. 3rd ACM Conference on Computer and Communications Security, März 1996, Neu Delhi, Indien.)

Eine Erweiterung des DH-Verfahren auf drei Teilnehmer A, B und C wird z. B. durch nachfolgende Tabelle beschrieben. (Berechnung jeweils mod p):

	$A \rightarrow B$	$B \rightarrow C$	$C \rightarrow A$
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der drei Teilnehmer den geheimen Schlüssel g^{abc} mod p berechnen.

Bei allen diesen Erweiterungen tritt mindestens eines der drei folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z. B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT`94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000 Bit gesendet werden müssen.
Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptografisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren soll das Etablieren eines gemeinsamen Gruppenschlüssels zwischen einer Zentrale und einer Gruppe von n Teilnehmern ermöglichen . Das Verfahren soll so ausgebildet werden, daß auch nach dem Etablieren des Gruppenschlüssels ohne großen Aufwand Teilnehmer aus dem Schlüsselverzeichnis gelöscht oder hinzugefügt werden können.

Die Aufgabenstellung wird durch eine Verfahren gelöst, bei welchem das Etablieren eines Gruppenschlüssels mit Hilfe einer Baumstruktur vorgenommen wird. Erfindungsgemäß wird dazu die Anzahl der an der Schlüsselvereinbarung beteiligten Teilnehmer n als binärer Baum mit n Blättern darstellen. Für jede natürliche Zahl n gibt es ein oder mehr

Darstellungen dieser Art. Die Anzahl der Blätter ist dabei mit der Anzahl der in das Verfahren einbezogenen Teilnehmer identisch. Das bedeutet, daß einer Anzahl von n Teilnehmern eine Anzahl von n Blätter eines binären Baumes mit der Tiefe $\lceil \log_2 n \rceil$ zugeordnet ist

Fig. 1 zeigt das Wirkprinzip des erfindungsgemäßen Verfahrens anhand der Baumstruktur einer Schlüsselvereinbarung für drei Teilnehmer A, B, C
Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B und C wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \bmod p$, der dem gemeinsamen Knoten K1 zugeordnet wird.
- Teilnehmer A und B auf der einen und Teilnehmer C auf der anderen Seite führen ein zweites DH-Verfahren durch, welches auf dem gemeinsamen Schlüssel k1 der Teilnehmer A und B und auf einer nach dem Zufallsprinzip generierten Zahl c des Teilnehmers C beruht. Das Ergebnis ist der gemeinsame Schlüssel $k=g^{kl \cdot c} \bmod p$, der der Wurzel des Baumes K_W zugeordnet wird.

Das erfindungsgemäße Verfahren wird anhand von Ausführungsbeispielen näher erläutert.
In Fig. 2 ist die Baumstruktur für eine Schlüsselvereinbarung für vier Teilnehmer A, B, C und D dargestellt.
Fig 3 zeigt die Baumstruktur einer Schlüsselvereinbarung für 5 Teilnehmer A, B, C, D und E.
Fig. 4 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach Fig.2, ein Beispiel für die Erweiterung der Baumstruktur um einen Teilnehmer.
Fig. 5 zeigt, ausgehend von einer bereits bestehenden Baumstruktur nach Fig. 2, das Entfernen/Löschen eines Teilnehmers aus der Baumstruktur.

Nachfolgend wird anhand von Figur 2 ein Beispiel einer Schlüsselvereinbarung für vier Teilnehmer A, B, C und D beschrieben:
Um einen gemeinsamen Schlüssel für vier Teilnehmer (Fig.2) zu etablieren, gehen Teilnehmer A, B, C und D wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit nach dem Zufallsprinzip generierten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \mod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2=g^{cd} \mod p$.
- Teilnehmer A und B auf der einen und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der Schlüssel k1 und von Teilnehmer C und D der Schlüssel k2 einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $k_W=g^{k1 \cdot k2} \mod p$, welcher der Wurzel des Baumes K_W zugeordnet ist.

Nachfolgend wird anhand von Figur 3 ein Beispiel einer Schlüsselvereinbarung für fünf Teilnehmer A, B, C, D, und E beschrieben:
Um einen gemeinsamen Schlüssel zu etablieren, gehen die Teilnehmer A, B, C, D und E wie folgt vor:

- Teilnehmer A und B führen ein DH-Verfahren mit zufällig gewählten Zahlen a und b durch. Sie erhalten den gemeinsamen Schlüssel $k1=g^{ab} \mod p$.
- Teilnehmer C und D führen ein DH-Verfahren mit zufällig gewählten Zahlen c und d durch. Sie erhalten den gemeinsamen Schlüssel $k2=g^{cd} \mod p$.
- Teilnehmer A und B auf der einen Seite und Teilnehmer C und D auf der anderen Seite führen gemeinsam ein zweites DH-Verfahren durch, in welches von Teilnehmer A und B der gemeinsame Schlüssel k1 und von Teilnehmer C und D der gemeinsame Schlüssel k2 einbezogen werden.. Das Ergebnis ist ein gemeinsamer Schlüssel $k3=g^{k1 \cdot k2} \mod p$ für die Teilnehmer A, B, C und D.
- Die Teilnehmer A, B, C und D auf der einen Seite und der Teilnehmer E auf der anderen Seite führen ein drittes DH-Verfahren durch, in welches der gemeinsame Schlüssel k3 der Teilnehmer A, B, C und D und eine für den Teilnehmer E generierte Zufallszahl e einbezogen werden. Das Ergebnis ist der gemeinsame Schlüssel $k_W=g^{k3 \cdot e} \mod p$, der der Wurzel des Baumes K_W zugeordnet ist.

Aufgrund der Struktur des erfindungsgemäßen Verfahrens ist es möglich, neue Teilnehmer mit einzubeziehen bzw. einzelne Teilnehmer auszuschließen, ohne das ganze Verfahren für jeden Teilnehmer noch einmal durchführen zu müssen.

Das Einfügen eines neuen Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern nach Fig. 4 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend Fig. 2 in welche eine neuer Teilnehmer bei Blatt B eingefügt werden soll. Bei Hinzunahme eines neuen Teilnehmers in eine bereits bestehende Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden zum Etablieren eines neuen gemeinsamen Schlüssels für n+1 Teilnehmer an einer geeigneten Stelle des binären Baumes (Blatt B vorgegeben) zwei neue Blätter B1 und B2 angefügt. Der neue Baum besitzt dann n+1 Blätter und die Tiefe $\lceil \log_2(n+1) \rceil$. Der bisher dem Blatt B zugeordnete Teilnehmer wird einem der neue Blätter B1 zugeordnet. Der neue Teilnehmer wird dem anderen noch freien Blatt B2 zugeordnet. Das bisherige Blatt B wird zu einem Knoten K1 für die Blätter B1 und B2. Ausgehend von den neuen Blättern B1 und B2 werden bis hin zur Wurzel des Baumes nur in den Knoten K neue Geheimnisse etabliert, die im Rahmen der Baumstruktur auf dem Weg von den neuen Blättern B1 und B2 zur Wurzel des Baumes K_W liegen. Das sind im konkreten Fall die Knoten K1, K2 und K_W.

Ist die Anzahl der Teilnehmer eine Zweierpotenz, so erhöht sich die Tiefe des Baumes durch diesen Vorgang um 1 (vgl. vorhergehendes Beispiel). Ist die Anzahl der Teilnehmer keine Zweierpotenz, so kann durch geschickte Wahl des aufzuteilenden Blattes eine Vergrößerung der Tiefe vermieden werden, wie das folgende Beispiel zeigt:

Um beispielsweise einen vierten Teilnehmer zu drei Teilnehmern hinzuzufügen, geht man (ausgehend von der Situation nach Fig.1) wie folgt vor:

- Teilnehmer C führt mit dem neu hinzugekommenen Teilnehmer D ein DH-Verfahren mit zufällig generierten Zahlen c` und d durch (c` sollte sich von dem vorher gewählten c unterscheiden, dies muß aber nicht der Fall sein). Das Ergebnis ist $k2` = g^{c`d} \bmod p$.
- Teilnehmer A und Teilnehmer B auf der einen und Teilnehmer C und D auf der anderen Seite führen ein DH-Verfahren mit den Werten k1 und k2` durch. Das Ergebnis ist $k = g^{k1 \cdot k2`} \bmod p$.

Bei einer derartigen Konfiguration müssen die Teilnehmer A und B keinen neuen Schlüsseltausch durchführen. Generell müssen nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des neuen Teilnehmers zur Wurzel K_W liegen.

Das Ausschließen bzw. Löschen eines Teilnehmers wird anhand einer Baumstruktur mit vier Teilnehmern anhand von Figur 5 näher erläutert: Ausgangssituation ist dabei eine Baumstruktur entsprechend Fig. 2, aus der Teilnehmer B entfernt werden soll.
Beim Ausschließen bzw. beim Löschen eines Teilnehmers B aus einer bereits bestehenden Baumstruktur, die über ein gemeinsames Geheimnis verfügt, werden wie in Fig. 5 ausgeführt, sowohl das Blatt des zu entfernenden Teilnehmers B als auch das Blatt des dem gleichen gemeinsamen Knoten K1 zugeordneten Teilnehmers A entfernt. Der gemeinsame Knoten K1 wird zum neuen Blatt A' des in der Baumstruktur verbleibenden Teilnehmers A. Ausgehend von den Blättern des Baumes bis zur Wurzel K_W werden nur in den Knoten K neue Geheimnisse etabliert, die vom neuen Blatt A' im Rahmen der Baumstruktur in Richtung Wurzel K_W unmittelbar tangiert werden. Das ist im konkreten Fall nur der Wurzelknoten K_W. Bei einer derartigen Konfiguration müssen die Teilnehmer C und D keinen neuen Schlüsseltausch durchführen. Generell müssen auch hier nur die Geheimnisse neu vereinbart werden, die im zugehörigen Baum auf dem Weg vom Blatt des Partners des entfernten Teilnehmers zur Wurzel liegen.

Das Verfahren kann in vielfacher Hinsicht zweckmäßig weiter ausgestaltet werden:
Für die Bildung der diskreten Exponentialfunktion $x \rightarrow g^x$ bietet sich beispielsweise die Verwendung anderer Gruppen an.
Beim Hinzufügen oder Entfernen eines Teilnehmers kann beispielsweise vereinbart werden, daß für die notwendigen neuen Durchführungen des DH-Verfahrens nicht die alten Geheimnisse, sondern das Ergebnis einer (evtl. randomisierten) Einwegfunktion verwendet wird.

(3) Patentansprüche:

1. Verfahren zum Etablieren eines gemeinsamen kryptografischen Schlüssels für n Teilnehmer unter Anwendung des DH-Verfahrens,
dadurch gekennzeichnet,
-daß jedem der n Teilnehmer (I) jeweils ein Blatt eines binär strukturierten Baumes, der genau n Blätter und die Tiefe $\lceil \log_2 n \rceil$ besitzt, zugeordnet wird,
-daß für jeden Teilnehmer (I) ein Geheimnis (i) generiert und dem Blatt des Baumes zugeordnet wird, dem auch der jeweilige Teilnehmer (I) zugeordnet ist,
-daß nacheinander in Richtung der Baumwurzel für alle Knoten (K) des Baumes Geheimnisse etabliert werden, wobei ausgehend von den Blättern entsprechend der festgelegten Baumstruktur über die gesamte Hierarchie der Baumstruktur immer zwei bereits bekannte Geheimnisse über das DH-Verfahren zu einem neuen gemeinsamen Geheimnis zusammengefaßt und einem gemeinsamen Knoten (K) zu geordnet werden, so daß der letzte Knoten K_W und damit die Baumwurzel, als Geheimnis den gemeinsamen Schlüssel aller n Teilnehmer enthält.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,**
-daß bei Aufnahme eines neuen Teilnehmers in eine bestehende Baumstruktur, die bereits über ein gemeinsames Geheimnis verfügt, zum Etablieren eines gemeinsamen Schlüssel für n+1 Teilnehmer an geeigneter Stelle des binären Baumes einem Blatt (B) als Nachfolger zwei neue Blätter (B1 und B2) angefügt werden, so daß der neue Baum genau n+1 Blätter und die Tiefe $\lceil \log_2(n+1) \rceil$ besitzt,
-daß der dem bisherigen Blatt (B) zugeordnete Teilnehmer und der neue Teilnehmer jeweils einem der neuen Blätter (B1; B2) zugeordnet werden, wobei das bisherige Blatt B zu einem gemeinsamen Knoten für die neuen Blätter (B1;B2) wird,
-daß ausgehend von den neuen Blättern (B1;B2) bis zur Wurzel des Baumes nur in den Knoten neue Geheimnisse etabliert werden, die im Rahmen der Baumstruktur auf dem Weg von den Blättern B1 und B2 zur Baumwurzel liegen.

3. Verfahren nach Anspruch 1, **d a d u r c h g e k e n n z e i c h n e t,**

-daß bei Ausschließung eines Teilnehmers (B) aus einer bereits bestehenden Baumstruktur die bereits über ein Geheimnis verfügt, sowohl das Blatt des zu entfernenden Teilnehmers (B), als auch daß Blatt des dem gleichen gemeinsamen Knoten zugeordneten Teilnehmers (A) entfernt werden,

-daß der gemeinsame Knoten zum Blatt des nicht zu entfernende Teilnehmers A wird, und daß ausgehend von den Blättern des Baumes bis zur Wurzel nur in den Knoten neue Geheimnisse ertabliert werden, die im Rahmen der Baumstruktur auf dem Weg vom neuen Blatt (A) zur Baumwurzel liegen.

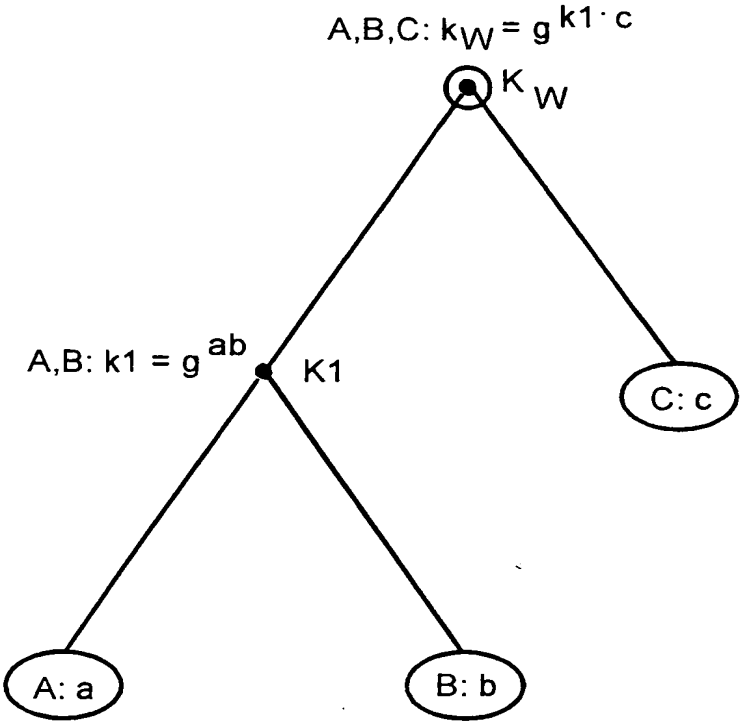


Fig. 1

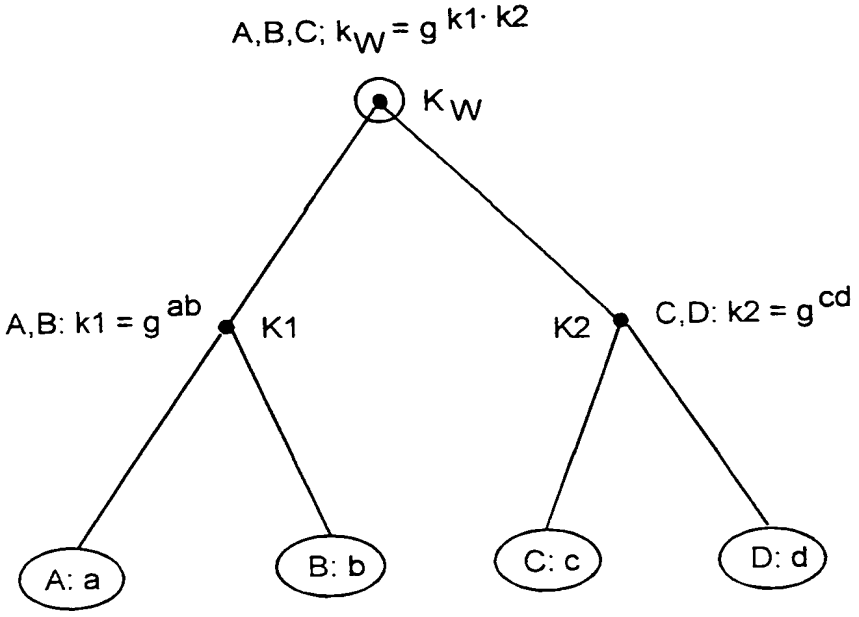

A,B,C; $k_W = g^{k1 \cdot k2}$
K_W
A,B: $k1 = g^{ab}$
K1
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 2

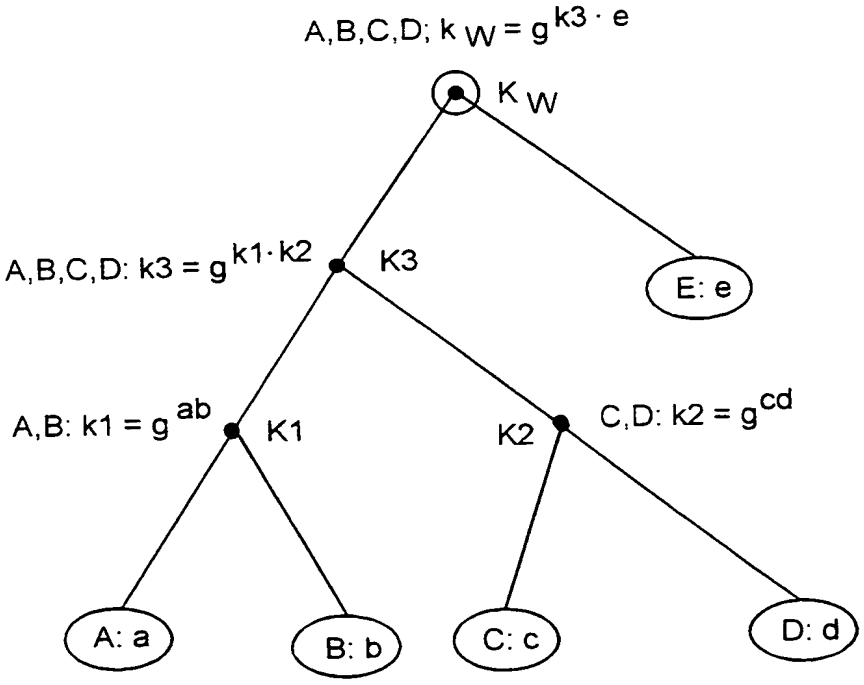

A,B,C,D; $k_W = g^{k3 \cdot e}$
K_W
A,B,C,D: $k3 = g^{k1 \cdot k2}$
K3
E: e
A,B: $k1 = g^{ab}$
K1
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 3

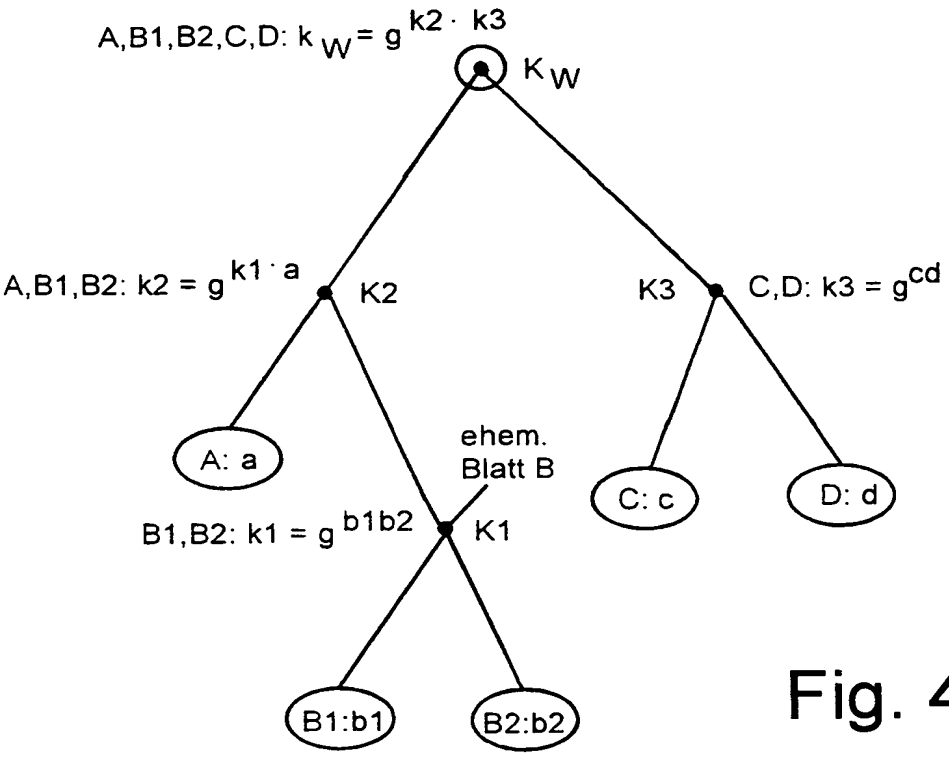

A,B1,B2,C,D: $k_W = g^{k2 \cdot k3}$
K_W
A,B1,B2: $k2 = g^{k1 \cdot a}$
K2
K3
C,D: $k3 = g^{cd}$
A: a
ehem. Blatt B
B1,B2: $k1 = g^{b1b2}$
K1
C: c
D: d
B1:b1
B2:b2

Fig. 4

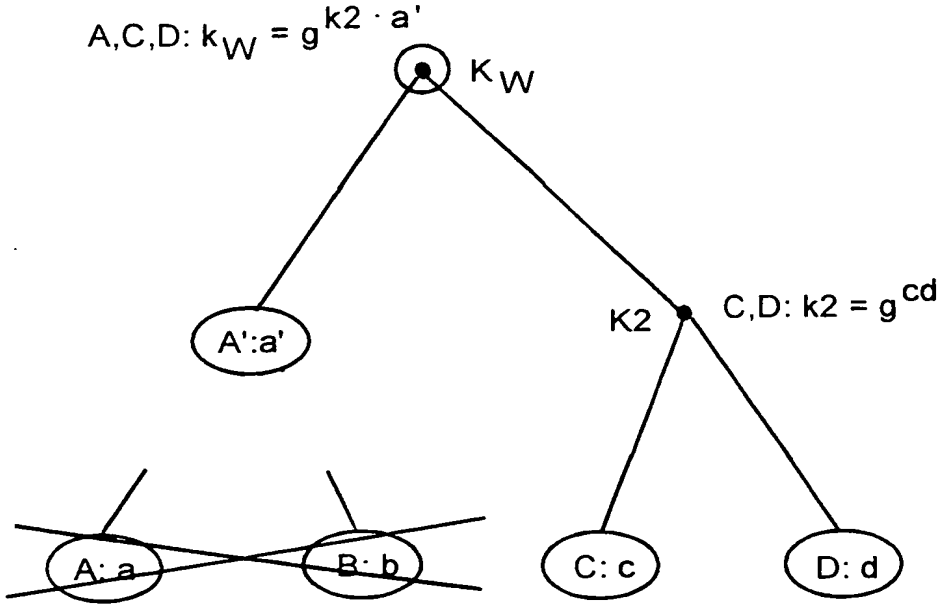

A,C,D: $k_W = g^{k2 \cdot a'}$
K_W
A':a'
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 5

INTERNATIONAL SEARCH REPORT

Inte. .onal Application No
PCT/EP 99/07051

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAVID A. MCGREW AND ALAN T. SHERMAN: "Key establishment in large dynamic groups using one-way function trees", 20. Mai 1998 (1998-05-20), Seiten 1-13 Verfügbar auf Internet: <http://www.cs.umbc.edu/{sherman/Papers/itse.ps> 23. Juni 1998 XP002126220 page 3 -page 4; figure 1 ---	1-3
A	DE 196 49 292 A (DEUTSCHE TELEKOM AG) 4 June 1998 (1998-06-04) column 3, line 23 -column 5, line 55; figure 1 --- -/--	1-3

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 December 1999	27/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Zucka, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 99/07051

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, pages 275-286, XP000852509 1995, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-60176-7 cited in the application page 278, last paragraph -page 279, paragraph 1 ---	1-3
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14-16 MARCH 1996,1996, pages 31-37, XP000620975 New York, NY, USA, USA ISBN: 0-89791-829-0 cited in the application page 34, column 2 -page 35, column 1 ---	1-3
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16 April 1997 (1997-04-16) cited in the application claim 1 ---	1
A	STEINER M ET AL: "CLIQUES: a new approach to group key agreement" PROCEEDINGS. 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (CAT. NO.98CB36183), PROCEEDINGS OF 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, AMSTERDAM, NETHERLANDS, 26-29 MAY 1998, pages 380-387, XP002126180 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8292-2 page 382, column 1, last paragraph -page 385, column 1 -----	1-3

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. ..ional Application No
PCT/EP 99/07051

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19649292 A	04-06-1998	NONE	
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999

M'H

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts P98136WO.IP	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/EP 99/07051	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 22/09/1999	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 09/10/1998
Anmelder DEUTSCHE TELEKOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Inte. .onales Aktenzeichen
PCT/EP 99/07051

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DAVID A. MCGREW AND ALAN T. SHERMAN: "Key establishment in large dynamic groups using one-way function trees", 20. Mai 1998 (1998-05-20), Seiten 1-13 Verfügbar auf Internet: <http://www.cs.umbc.edu/{sherman/Papers/itse.ps> 23. Juni 1998 XP002126220 Seite 3 -Seite 4; Abbildung 1 ---	1-3
A	DE 196 49 292 A (DEUTSCHE TELEKOM AG) 4. Juni 1998 (1998-06-04) Spalte 3, Zeile 23 -Spalte 5, Zeile 55; Abbildung 1 --- -/--	1-3

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Dezember 1999	27/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Zucka, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07051

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, Seiten 275-286, XP000852509 1995, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-60176-7 in der Anmeldung erwähnt Seite 278, letzter Absatz -Seite 279, Absatz 1 ---	1-3
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14-16 MARCH 1996,1996, Seiten 31-37, XP000620975 New York, NY, USA, USA ISBN: 0-89791-829-0 in der Anmeldung erwähnt Seite 34, Spalte 2 -Seite 35, Spalte 1 ---	1-3
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16. April 1997 (1997-04-16) in der Anmeldung erwähnt Anspruch 1 ---	1
A	STEINER M ET AL: "CLIQUES: a new approach to group key agreement" PROCEEDINGS. 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (CAT. NO.98CB36183), PROCEEDINGS OF 18TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, AMSTERDAM, NETHERLANDS, 26-29 MAY 1998, Seiten 380-387, XP002126180 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8292-2 Seite 382, Spalte 1, letzter Absatz -Seite 385, Spalte 1 -----	1-3

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 99/07051

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19649292 A	04-06-1998	KEINE	
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999